

What is claimed is:

1 1. A method for providing access to secure data through a portable computing
2 system during a specified time, wherein said method comprises:
3 establishing a connection between said portable computing system and a
4 base computing system to provide for transfer of data between said portable
5 computing system and said base computing system;
6 verifying identity of said base computing system within said portable
7 computing system;
8 resetting a timer within said portable computing system to run for a specified
9 time; and
10 providing access to said secure data only when said timer is running.

1 2. The method of claim 1, wherein said step or verifying identity of said base
2 computing system comprises:
3 receiving and storing a public cryptographic key from said base computing
4 system during an initialization process,
5 following said initialization process, generating a random number within said
6 portable computing system;
7 transmitting said random number to said base computing system;
8 receiving a number transmitted from said base computing system;
9 decrypting said number transmitted from said base computing system to form
10 a decrypted number; and
11 determining that said decrypted number matches said random number.

1 3. The method of claim 1, additionally comprising a step of verifying whether a
2 password is entered correctly in said portable computing system.

1 4. The method of claim 3, wherein said step of verifying whether a password is
2 entered correctly includes:

3 transmitting an initial password to said base computing system during an
4 initialization process,

5 storing said initial password within said base computing system;

6 following said initialization process, transmitting a present password to said
7 base computing system;

8 determining in said base computing system that said initial password
9 matches said present password;

10 transmitting an approval code from said base computing system to said
11 portable computing system; and

12 determining that said approval code has been received.

1 5. The method of claim 1, wherein said connection is established through a
2 switched telephone network.

1 6. The method of claim 1, wherein

2 said timer includes a timer register storing a number corresponding to a time
3 remaining,

4 said number corresponding to a time remaining is decremented in response
5 to a series of timing pulses generated within said portable computing system, and

6 setting said timer includes storing a number corresponding to said specified
7 time in said timer register.

1 7. A method providing for access to secure data through a portable computing
2 system, wherein said access to said secure data is limited to a specified time, and
3 wherein said method comprises:

4 initializing a base computing system and said portable computing system to
5 work together as a system by an initialization process comprising storing data
6 identifying said base computing system within said portable computing system; and

RPS9-2001-0049-US1

7 resetting said portable computing system by a reset process following said
8 initialization process including:
9 establishing a connection to transmit data between said portable
10 computing system and a base computing system;
11 determining, using said data identifying said base computing system,
12 that said connection has been made between said portable computing
13 system and said base computing system;
14 setting a timer within said portable computing system to run until said
15 specified time has expired;
16 determining if said timer is running; and
17 providing access to said secure data only when said timer is running.

1 8. The method of claim 7, wherein
2 said initialization process additionally includes determining whether said data
3 identifying a base computing system has been previously stored in said portable
4 computing system;
5 if said data identifying a base computing system is determined to have been
6 previously stored, said data identifying a base computing system remains without
7 being overwritten during said initialization process.

1 9. The method of claim 8, wherein said data identifying said base computing is
2 a public cryptographic key of said base computing system, and wherein said
3 process of determining that said connection has been made between said portable
4 computing system and said base computing system includes:

5 generating and storing random number within said portable computing
6 system;

7 transmitting said random number from said portable computing system to
8 said base computing system;

9 encrypting said random number within said base computing system with a
10 private cryptographic key of said base computing system to form an encrypted
11 number;

12 transmitting said encrypted number from said base computing system to said
13 portable computing system;

14 decrypting said encrypted number within said portable computing system with
15 said public cryptographic key of said base computing system to form a decrypted
16 number; and

17 comparing said decrypted number with said random number stored within
18 said portable computing system.

1 10. The method of claim 8, wherein

2 said timer includes a timer register storing a number corresponding to a time
3 remaining,

4 said number corresponding to a time remaining is decremented in response
5 to a series of timing pulses generated within said portable computing system, and

6 setting said timer includes storing a number corresponding to said specified
7 time in said timer register.

1 11. The method of claim 8, wherein
2 said method additionally comprises receiving an input corresponding to a
3 time, and
4 setting said specified time according to said input.

1 12. The method of claim 8, additionally comprising storing a cryptographic public
2 cryptographic key of said portable computing system within said base computer
3 system.

1 13 The method of claim 8, wherein
2 said initialization process additionally includes receiving a present password
3 as an input, determining if a password has been previously stored, and storing said
4 present password in response to a determination that said password has not been
5 previously stored, and

6 said reset process additionally includes receiving a present password as an
7 input and determining if said password matches a stored password;

8 said timer is set within said portable computing system only in response to
9 a determination that said password matches said stored password.

1 14. The method of claim 13, wherein
2 said present password is received as an input within said portable computing
3 system,

4 said present password is transmitted from said portable computing system
5 to said base computing system,

6 said present password is stored within said base computing system following
7 a determination that a password is not previously stored within said base computing
8 system;

9 a determination is made in said base computing system of whether said
10 present password matches a stored password,

11 said reset process additionally includes transmitting an approval code from
12 said base computing system to said portable computing system in response to a
13 determination that said present password matches said stored password, and
14 said timer is set within said portable computing system in response to
15 receiving said approval code.

1 15. The method of claim 14, wherein said data identifying said base computing
2 is a public cryptographic key of said base computing system, and wherein
3 said process of determining that said connection has been made between said
4 portable computing system and said base computing system includes:

5 generating and storing random number within said portable computing
6 system;

7 concatenating said random number and said present password within said
8 portable computing system to form a concatenated number;

9 encrypting said concatenated number within said portable computing system
10 with said public cryptographic key of said base computing system to form a first
11 encrypted number;

12 transmitting said first encrypted number from said portable computing system
13 to said base computing system;

14 decrypting said first encrypted number within said base computing system
15 with a private cryptographic key of said base computing system to form a decrypted
16 number;

17 dividing said decrypted number to form a decrypted random number and said
18 present password;

19 encrypting said decrypted random number within said base computing
20 system with a private cryptographic key of said base computing system to form a
21 second encrypted number;

22 transmitting said second encrypted number from said base computing
23 system to said portable computing system;

24 decrypting said second encrypted number within said portable computing

RPS9-2001-0049-US1

25 system with said public cryptographic key of said base computing system to form
26 a decrypted number; and
27 comparing said decrypted number with said random number stored within
28 said portable computing system.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

1 16. A system for providing controlled access to secure data, wherein said system
2 comprises:

3 a portable computing system providing said controlled access to secure data
4 during a specified time, wherein said portable computing system includes first
5 processing means, first storage means, and a timer;

6 a base computing system including second processing means and second
7 storage means;

8 a connection between said portable computing system and said base
9 computing system for transmitting data between said portable computing system
10 and said base computing system; and

11 a first program, executing within said first processing means, causing said
12 portable computing system to perform a process including:

13 determining if a public cryptographic key is stored in a first location
14 within said first storage means;

15 in response to determining that a public cryptographic key is not
16 stored in said first location, transmitting a request code, receiving said public
17 cryptographic key, and storing said public cryptographic key in said first
18 location;

19 transmitting a first code;

20 receiving a response to said first code;

21 determining from said response to said first code if a connection has
22 been made to said base computing system; and

23 setting said timer to run until said specified time has expired;

24 a subroutine executing within said first processing means, causing said
25 portable computing system to perform a process including:

26 determining if said timer is running; and

27 providing access to said secure data only when said timer is running;

28 and

29 a second program, executing within said second processing means, causing

said base computing system to perform a process including:
receiving said request code;
in response to receiving said request code, transmitting a public cryptographic key of said base computing system to said portable computing system;
receiving said first code; and
in response to receiving said first code, transmitting said response to said first code.

17. The system of claim 16, wherein
said first storage means includes a timer register storing a number corresponding to a time remaining,
said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and
setting said timer includes storing a number corresponding to said specified time in said timer register.

18. The system of claim 17, wherein
said step of transmitting a first code includes generating a random number, storing said random number in a second location within said first storage, and transmitting said random number to said base computing system as said first code,
said step of transmitting said response to said first code includes encrypting said random number with a private cryptographic key of said base computing system to form an encrypted random number, and transmitting said encrypted random number as said response to said portable computing system as said response to said first code, and
said step of determining from said response to said first code if a connection has been made to said base computing system includes decrypting said encrypted number to form a decrypted number and comparing said decrypted number with said random number stored in said second location within said first storage.

1 19. The system of claim 18, wherein
2 said first processing means includes a first microprocessor and a first
3 cryptographic processor,
4 said encrypted number is decrypted in said first cryptographic processor,
5 said first storage means includes first secure storage accessed only through
6 said first cryptographic processor, and
7 said first location and said timer register within said first storage means are
8 within said secure storage.

1 20. The system of claim 18, wherein
2 said second processing means includes a second microprocessor and a
3 second cryptographic processor,
4 said random number is encrypted to form said encrypted number within said
5 second cryptographic processor,
6 said second storage means includes second secure storage accessed only
7 through said second cryptographic processor, and
8 said private cryptographic key of said base computing system is stored within
9 said second secure storage.

1 21. The system of claim 16, wherein
2 said portable computing system additionally includes a display,
3 said first program additionally causes a successful completion message to
4 be displayed on said display in response to a determination from said response to
5 said first code that a connection has been made to said base computing system,
6 and
7 said first program additionally causes an error message to be displayed on
8 said display in response to a determination from said response to said first code
9 that a connection has not been made to said base computing system.

1 22. The system of claim 16, wherein
2 said portable computing system additionally includes a display and a
3 keyboard, and
4 said first program causes said portable computing to perform a process
5 additionally including displaying a menu, receiving a user input from said keyboard
6 as said menu is displayed, and determining said specified time from said user input.

1 23. The system of claim 16, wherein
2 said portable computing system additionally includes a display and a
3 keyboard,
4 said first program causes said portable computing to perform a process
5 additionally including displaying a menu and receiving a password from said
6 keyboard as said menu is displayed,
7 said step of transmitting a first code includes:
8 generating a random number;
9 storing said random number in a second location within said first
10 storage;
11 concatenating said random number with said password to form a
12 concatenated number,

13 encrypting said concatenated number with a private cryptographic key
14 of said portable computer system stored in a third location within said first
15 storage means to form said first code; and
16 transmitting said random number to said base computing system as
17 said first code,
18 said step of transmitting said response to said first code includes:
19 decrypting said first code with a private cryptographic key of said base
20 computing stored in a fourth location within said second storage means;
21 separating said password from said random number;
22 determining whether said password separated from said random
23 number matches a password stored;
24 encrypting said random number with a private cryptographic key of
25 said base computing system to form an encrypted random number, and
26 determining if and transmitting said encrypted random number as said
27 response to said portable computing system as said response to said first
28 code,
29 said second program causes said base computing system to perform a
30 process additionally including:
31 determining if a password is stored in a fifth location within said
32 second storage means;
33 in response to a determination that a password is not stored in said
34 fifth location, storing said password separated from said random number in
35 said fifth location;
36 in response to a determination that a password is stored in said fifth
37 location, comparing said password stored in said fifth location with said
38 password separated from said random number;
39 in response to determining that said password stored in said fifth
40 location matches said password separated from said random number,
41 encrypting said random number and to form a transmitting an approval code
42 to said portable computing system as said response to said first code; and

43 said step of determining from said response to said first code if a connection
44 has been made to said base computing system includes determining that said
45 approval code has been received.

1 24. The system of claim 23, wherein

2 said second program causes said base computing system to perform a
3 process additionally including, in response to determining that said password stored
4 in said fifth location does not match said password separated from said random
5 number, transmitting an error code to said portable computing system as said
6 response to said first code

7 said first program causes said portable computing to perform a process
8 additionally including displaying a successful completion message on said display
9 in response to receiving said approval code, and displaying an error message on
10 said display in response to receiving said error code.

1 25. The system of claim 23, wherein

2 said first storage means includes a timer register storing a number
3 corresponding to a time remaining,

4 said number corresponding to a time remaining is decremented in response
5 to a series of timing pulses generated within said portable computing system, and

6 setting said timer includes storing a number corresponding to said specified
7 time in said timer register.

1 26. The system of claim 23, wherein

2 said first processing means includes a first microprocessor and a first
3 cryptographic processor,

4 said concatenated number is encrypted in said first cryptographic processor,

5 said first storage means includes first secure storage accessed only through
6 said first cryptographic processor, and

7 said secure storage includes said first location, said third location, and said

8 timer register within said first storage means.

1 27. The system of claim 23, wherein

2 said second processing means includes a second microprocessor and a
3 second cryptographic processor,

4 said random number is encrypted to form said encrypted number within said
5 second cryptographic processor,

6 said second storage means includes second secure storage accessed only
7 through said second cryptographic processor, and

8 said fourth and fifth locations within said second storage means are within
9 said second secure storage.

1 28. The system of claim 23, wherein

2 said step of transmitting a request code includes transmitting a public
3 cryptographic key of said portable computing system, and

4 said step of receiving a request code includes storing said public
5 cryptographic key of said portable computing system in a sixth location within said
6 second storage means.

1 29. A computer readable medium within a portable computing system, wherein
2 said computer readable medium has computer readable instructions for performing
3 a method comprising:

4 determining if a public cryptographic key is stored in a first location within
5 said first storage means;

6 in response to determining that a public cryptographic key is not stored in
7 said first location, transmitting a request code, receiving said public cryptographic
8 key, and storing said public cryptographic key in said first location;

9 transmitting a first code;

10 receiving a response to said first code;

11 determining from said response to said first code if a connection has been

made to a base computing system; and
setting a timer to run until a specified time has expired.

30. The computer readable medium of claim 29, wherein said step of setting aid timer includes storing a number corresponding to said specified time in a timer register.

31. The computer readable medium of claim 29, wherein
said step of transmitting a first code includes generating and storing a random number, and transmitting said random number to said base computing system as said first code, and
said step of determining from said response to said first code if a connection has been made to a base computing system includes decrypting an encrypted number to form a decrypted number and comparing said decrypted number with said random number.

32. The computer readable medium of claim 29, wherein said method additionally comprises:
displaying a successful completion message in response to receiving an approval code; and
displaying an error message in response to receiving an error code.

33. The computer readable medium of claim 29, wherein said method additionally comprises:
displaying a menu;
receiving an input from a keyboard as said menu is displayed; and
determining said specified time from said input.

34. The computer readable medium of claim 29, wherein
said method additionally includes displaying a menu and receiving a

3 password from a keyboard as said menu is displayed,
4 said step of transmitting a first code includes:
5 generating a random number;
6 storing said random number in a second location within said first
7 storage;
8 concatenating said random number with said password to form a
9 concatenated number,
10 encrypting said concatenated number with a private cryptographic key
11 of said portable computer system stored in a third location within said first
12 storage means to form said first code; and
13 transmitting said random number to said base computing system as
14 said first code.

1 35. In a portable computing system having a user interface including a display
2 and a keyboard, a method for limiting access to secure data to a specified time,
3 wherein said method comprises:
4 displaying a screen location for entering a number;
5 accepting an input from said keyboard;
6 displaying said input from said keyboard in said screen location;
7 calculating a number determining said specified time as a function of said
8 input from said keyboard;
9 generating a random number;
10 transmitting said random number to a base computing system;
11 receiving an encrypted number from said base computing system,
12 decrypting said encrypted number with a public cryptographic key stored
13 within said portable computing system to form a decrypted number;
14 determining if said random number matches said decrypted number; and
15 in response to determining that said random number matches said decrypted
16 number, setting a timer within said portable computing system to run for said
17 specified time, wherein said access to secure data is provided only when said time

RPS9-2001-0049-US1

18 is running.

1 36. The method of claim 35, additionally comprising:

2 displaying a successful completion message in response to determining that
3 said random number matches said decrypted number; and

4 displaying an error message in response to determining that said random
5 number does not match said decrypted number.

1 37. In a portable computing system having a user interface including a display
2 and a keyboard, a method for limiting access to secure data to a specified time,
3 wherein said method comprises:

4 displaying a first screen location for entering a password and a second
5 screen location for entering a number;

6 accepting a first input from said keyboard;

7 generating a password from said first input;

8 accepting a second input from said keyboard;

9 displaying said input from said keyboard in said second screen location;

10 calculating a number determining said specified time as a function of said
11 second input from said keyboard;

12 generating a random number;

13 encrypting said password with a public cryptographic key stored in said
14 portable computing system;

15 transmitting said random number to a base computing system;

16 receiving an encrypted number from said base computing system,

17 decrypting said encrypted number with said public cryptographic key stored
18 within said portable computing system to form a decrypted number;

19 determining if said random number matches said decrypted number; and

20 in response to determining that said random number matches said decrypted
21 number, setting a timer within said portable computing system to run for said
22 specified time, wherein said access to secure data is provided only when said time

RPS9-2001-0049-US1

23 is running.

1 38. The method of claim 35, additionally comprising:
2 displaying a successful completion message in response to determining that
3 said random number matches said decrypted number; and
4 displaying an error message in response to determining that said random
5 number does not match said decrypted number and in response to receiving an
6 error code from said base system.

7

11/11/2019 11:11:11 AM